REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Applicant advises that in the cover page of the Office Action dated October 18, 2005 indicates that the drawings filed on July 16, 2001 are unacceptable. However, there is no discussion of such objections, and in fact, the cover page of the Office Action dated December 27, 2004 actually indicates that the drawings filed July 16, 2001 are acceptable. Applicant believes that the Office Action dated October 18, 2005 contains an error. Since Applicant has been given no guidance as to why the drawings are allegedly unacceptable, Applicant has not amended the drawings nor supplied replacement sheets at this time.

Objections to the Specification

The passage: "The secure module can be adapted to be removably coupled to the personalized device" added in the amendment filed May 27, 2005 has been rejected under 35 U.S.C. 132(a) for introducing new matter. Applicant respectfully traverses the rejection as follows.

In the May 27, 2005 amendment, Applicant advises that the above-mentioned passage was originally present in the application as filed as part of claim 12.

In establishing a disclosure, an applicant may rely not only on the description and drawings as filed, but also on the original claims if their content justifies it. Where subject matter not shown in the drawing or described in the description is claimed in the application as filed, and such original claim itself constitutes a clear disclosure of this subject matter, then the claim should be treated on its merits, and requirement made to amend the drawing and description to show this subject matter. The claim should not be attacked either by objection or rejection because this subject matter is lacking in the drawing and description. It is the drawing and description that are defective, not the claim. (see MPEP 608.01(l))

Applicant respectfully submits that claim 12 as originally filed constitutes a clear disclosure of the subject matter added, and as such it was the description that was defective, not the claim. Accordingly, Applicant has thus amended the description to include the subject matter originally disclosed in the claim, which is believed to be acceptable in view in MPEP 608.01(l).

Accordingly, Applicant believes that the above-noted subject matter should be allowed to be added to the description, and has not removed same in this response.

The Examiner objects to the numeral 30 found on page 6, line 24. Applicant advises that this issue was dealt with in the response filed May 27, 2005 (see page 2 of Applicant's response). The numeral "30" on line 24 was replaced with the numeral "24" to correct the discrepancy. Applicant respectfully submits that this objection has been previously overcome.

Claim Rejections – 35 U.S.C. §102

Claims 1,2, 4-12 have been rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,917,913 to Wang. Applicant respectfully traverses the Examiner's rejections as follows.

The present application describes and claims a method for verifying data integrity in cryptographic schemes. As exemplified in the description, at least one correspondent in a cryptographic scheme uses a personalized device that has a main processor and a secure module. The secure module is adapted to operate independently of the main processor so that the internal state of the secure module can not be readily reverse engineered and/or that its interactions with the underlying hardware are not maliciously intercepted and reinterpreted (see page 6, line 14-19).

An exemplary method is outlined in the description on page 7, lines 14-26. Data that is to be verified is assembled, and two separate outputs are displayed, one by the main processor and one by the secure module. The secure module is then only instructed to generate a signature upon a favourable comparison of the two outputs. Since the two outputs are operably independent, a favourable comparison indicates data integrity to an entity who wishes to verify the integrity. Independent claim 1 provides a method with such features.

Wang teaches a method in a portable electronic authorization device for approving a transaction request originated from an electronic transaction system. The method includes receiving a first set of digital data at the portable electronic authorization device, wherein the first set of digital data represents the transaction request. The method then includes transmitting

a second set of digital data to the electronic transaction system if the transaction request is approved by a use of the portable electronic authorization device. The second set of digital data is encrypted by an appropriate module in the portable electronic authorization device that signifies the user's approval of the transaction request.

Therefore, Wang teaches a single output, which is approved by a user before being sent to the electronic transaction system. Wang does not teach generating, displaying, or comparing two outputs to determine data integrity before approving the transaction. There is only a single output, sent along a single path.

The Examiner has relied on several passages from Wang in rejecting claim 1. Applicant will step through various steps and/or features recited claim 1 and compare such steps of features thereof to the particular passage(s) which have been applied by the Examiner.

Firstly, the preamble of claim 1 requires a secure module independently operative of a main processor. Presumably, the Examiner equates the "at least one correspondent" recited in claim 1 to the PEAD of Wang. As clearly shown in Figure 3A, the PEAD has only a single processor, namely encryption logic 300. Therefore, at most, Wang teaches a secure module or a main processor, and in fact, Figure 3A seems to indicate that logic 300 comprises both a processor and a secure module in the same component, and thus such features are not independently operative of each other. In the present invention, the secure module is independent of the main processor, e.g., to maintain secrecy of sensitive information whilst not requiring the entire processing capabilities of the correspondent to be secure. Clearly Wang does not teach a secure module independently operable of a main processor, but rather teaches a single secure module (200). Therefore, for at least that reason, Wang cannot anticipate claim 1.

Secondly, claim 1 requires that a first output is displayed under control of the main processor. The first output is then forwarded to the secure module, and the secure module displays the data as a second output to permit comparison of the first and second outputs. The Examiner refers to col. 4, lines 17-21 and 41-44 or col. 2 lines 18-23 and col. 10, line 66 through col.1 line 5. In col. 4, however at lines 25-30, Wang teaches a requesting device sending data pertaining to a transaction to the PEAD, via path 206 shown in Figure 2. As described in col. 4 lines 41-44, the user may then review the data pertaining to the transaction on either a screen

provided by the requesting device or a display screen on the PEAD. Therefore, at most, Wang teaches a first output on a single display. Wang does not teach two outputs, nor the comparison of such outputs, in fact Wang is entirely silent as to utilizing a pair of outputs. Claim 1 requires two separate outputs, displayed by two separate (and independently operative) devices (main processor and secure module). Wang simply does not teach such a feature. In fact, it is clear from the teachings of Wang relied upon by the Examiner that Wang uses only a single output, and there is no comparison of such an output with a second output. Therefore, for at least this reason, claim 1 cannot be anticipated by Wang.

Wang uses a PEAD to provide transaction approvals, such that identification data and/or a private key need not be stored by a requesting device (see col. 5, lines 50-55). Wang does not have a device with a separate main processor and secure module. Such separation, and the fact that these features belong to one correspondent, is clearly recited in claim 1. Each feature displays a separate output, and the comparison of the two outputs is made in order to determine whether a signature on the data should be made. Wang is entirely silent to a pair of outputs and in fact clearly intends to use the PEAD as only the means for approving the transaction. Since the PEAD does not provide a separate main processor, and secure module, and does not provide two displays nor a comparison of two outputs, Wang cannot anticipate claim 1.

Accordingly, Applicant respectfully submits that Wang does not teach every element of claim 1, and as such cannot anticipate claim 1.

Claims 2-9 being ultimately dependent on claim 1 are also believed to distinguish over Wang.

Applicant advises that claims 10 and 12 also require the comparison of two outputs, and as such arguments with respect to claim 1 equally apply thereto. Therefore Wang cannot anticipate claims 10 and 12. Claim 11, being dependent on claim 10 is also believed to distinguish over Wang.

Claim Rejections - 35 U.S.C. §103(a)

Claim 3 has been rejected under 35 U.S.C. §103(a) as being unpatentable over Wang in view of WO 00/54457 to Vatanen. Applicant respectfully traverses the rejections as follows.

Claim 3 is ultimately dependent on claim 1, and it has been shown above that Wang cannot anticipate claim 1. Therefore, Vatanen must not only teach what is recited in claim 3, but

also what is missing from Wang.

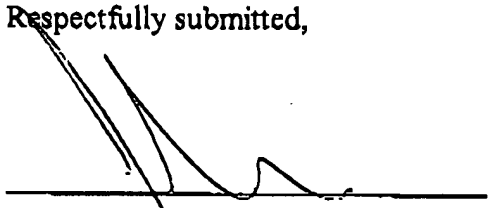
Although Vatanen does teach a mobile phone telecommunication system, Vatanen does not provide independently operative main processor and secure module that each display separate outputs to permit comparison of the outputs. Therefore, for at least that reason, Vatanen does not teach what is missing from Wang, and as such claim 3 is patentable over the combination of Wang and Vatanen.

Summary

In view of the foregoing, Applicant respectfully submits that claims 1-12 clearly and patentably distinguish over the prior art cited by the Examiner, and that all formal grounds for rejection have been addressed.

Accordingly, Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: December 14, 2005

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.3164
JRO/BSL